Defense Advanced Research Projects Agency (DARPA)
Information Resources Directorate (IRD)

Attachment No. 1

Statement of Work (SOW)

Table of Contents

.

Contract Title: Information Technology Services for the Defense Advanced Research Projects Agency (DARPA)

Contract Number: HR0011-05-R-0002

Fiscal Years: 1 year base (CY06) with 4 option years (FY 07 – 10)

1.0 Introduction

This is a statement of work for information technology seats and services for the Defense Advanced Research Projects Agency (DARPA). DARPA is located at 3701 North Fairfax Drive, Arlington, VA 22203-1714 and in other buildings nearby. The DARPA mission is to maintain U.S. technological superiority over potential adversaries by identifying and supporting breakthrough technologies of interest to the military. Information technology services in support of this responsibility require state-of-the-art tools and services, and rapid, flexible response to mission essential and evolving customer requirements. The Information Resources Directorate (IRD) of DARPA will manage this contract. The contractor may during the period of performance of this contract and for one year after, be excluded from competition for, and award of, any contractual arrangements, other than the re-competition of this contract, as prime contractor, subcontractor, partner, or in any other capacity for the Defense Advanced Research Projects Agency without the express written approval of the Contracting Officer. The contractor's employees shall be required to submit the Non-Disclosure Agreement included in Section J as Attachment 13 of the basic contract. The intent of this provision is to prevent a situation in which a company who has unlimited access to DARPA information (acquisition, budget, project plans, etc.) is able to bid on future DARPA work where information regarding that work would provide an unfair competitive advantage. Offerors who may have a potential conflict of interest under this clause should request a review by the contracting officer. Requests for such reviews should be submitted to the contracting officer in writing and include: Name of company, current DARPA contract number, role of the contractor (prime or sub), nature of the work performed, and a description of the current level of access to DARPA facilities and information.

1.1 Background

The statement of work for the incumbent contractor (RS Information Systems, Inc) is provided in Section J Attachment 10 for informational purposes only. Section J-Attachment 11 is a list of projects currently being performed by the incumbent contractor. The successful contractor shall assume ownership of all currently deployed assets at a cost as delineated in the incumbent contractor's credit/asset report at the time of the contract award. The current credit/asset report is included in Section J as Attachment 9. The IT Configuration Control Governance Structure is provided in Section J as Attachment 7. Legacy Systems are listed in Section J as Attachment 6. The incumbent services contractor is working under a full performance contract option that expires on 31 December 2005. DARPA plans to award the base year task under this contract to

commence in mid-December 2005. To effect transition from the incumbent to the successful Offeror, DARPA will award a contract option to the incumbent to transition to the successful Offeror. Section J, Attachment 8 contains a listing of all current DARPA seat types, network and telecommunications services and configurations supported by the incumbent. DARPA anticipates providing government-furnished space which includes all furniture, equipment, telephone services, office supplies, etc. needed for the performance of this contract as follows: 1,269 total sq. ft at 3701 North Fairfax Dr., comprised of 272 sq. ft. for a customer service area, 540 sq. ft. for on-site Help Desk support, 240 sq. ft. for the NOC and 217 sq. ft. of conditioned computer room space. The Contractor shall be responsible for procuring all other space necessary to deliver the services detailed in this statement of work.

2.0 Objectives

DARPA envisions that the successful Offeror shall provide and manage the full range of classified information technology service, support, and infrastructure necessary to implement the DARPA information technology strategic direction and operational objectives, which are expected to evolve over the course of this task order. DARPA envisions that the government staff will focus on inherently governmental functions to include articulating mission requirements to the contractor, strategic planning, capital planning, information assurance policy and oversight, independent verification and validation, and performance monitoring. DARPA may use other government or commercial third parties to advise and/or assist in performing its responsibilities.

DARPA secure IT services consists of stand alone systems, closed LANs, Agency-wide or common use networks and small file transfer networks (in progress). The primary objective during the base year is to deploy a system that shall incorporate the stand-alone systems and internal LANs into a single Agency-wide network serving multiple offices, programs and remote terminals. This consolidation will allow DARPA to more effectively manage closed LANs and removable hard drives. By the end of the second option, the network will increase functionally to include interfaces with other DoD managed networks.

Throughout the course of the contract, existing Agency-wide or common use networks and special purpose systems, need to be operated and managed by the IT service provider. As DARPA's classified requirements grow and continue to change, all classified IT services will be provided by the contractor.

Information Technology services provided under this statement work is essential to the accomplishment of DARPA's mission. DARPA has been and expects to be in the foreseeable future, a multi-platform environment. It is critical that continuity of operations and services be maintained at the current full performance level during the period of transition from the incumbent contractor to the successful Offeror. To minimize the risk inherent in transition DARPA will proactively facilitate the transfer of explicit and tacit knowledge, methods, and procedures from the DARPA staff and the incumbent contractor staff to the successful Offeror. The provisions of FAR 52.237-3(c) apply. To create an environment for successful transition,

DARPA envisions that this statement of work will be accomplished in a manner that provides an orderly 'ramp up' for the successful Offeror and an orderly 'ramp down' for the incumbent contractor.

3.0 Scope

This Statement of Work establishes the basic requirements related to providing classified office computing, networking, and communications service and technical support to DARPA. This statement of work consists of the following sections:

- DARPA Service Delivery Points (SDPs)
- Customer Information Technology (IT) Services
- Information Assurance/Computer Network Defense (IA/CND) Services
- Catalog Services
- Expert Assistance Tasks
- Governance
- Transition Services

Work identified in this document shall meet the levels of service specified in Section C-4 of the basic contract, Service Level Objectives (SLOs). Services in this contract are 24 x 7, however the predominant amount of service tickets are generated during DARPA's core hours between 7am and 7pm, Monday through Friday.

All DARPA information resources and contractor generated data such as system log data, documentation, program code, automated scripts and ancillary information under the contract is owned by the Government. As such, the contractor must allow and provide capabilities for authorized Government managers and staff, as well as designated contractors' access to such data. Authorized DARPA staff and contractors shall have full and unrestricted access to such data. Upon request by DARPA, the contractor shall, without delay, deliver and convey any/all requested DARPA files/documents, etc. to the appropriate DARPA person or organization. Likewise, the contractor must provide on-going direct systems/automated access to DARPA files and databases. Such direct systems access shall include admin or root type access for the purpose of oversight. Management consoles must be accessible for validation/monitoring purposes. Deliverables required by the contract are government property and may be redistributed within the Agency for management or verification purposes.

The contractor shall demonstrate that the proposed PL/3 and future PL/4 solutions required by this contract has been previously accredited and has wide acceptance in both the SAP and SCI communities.

4.0 Definitions

For the purposes of this document, the following definitions apply:

Accredited means that a system or facility has been granted authority to operate by the Designated Approval Authority of a government agency or entity (e.g., DIA) and/or the Director, Security and Intelligence/DAA, DARPA, based on accreditation requirements specified by appropriate DoD or DCI documents.

Appropriate Security Features – see Necessary Security Features

Assurance refers to availability, restricted access/confidentiality, integrity/data quality, attack/intrusion detection time, and attack termination time.

Capacity refers to ubiquity of access, connectivity, redundancy/diversity, compute capacity, committed information rate/peak information rate, and growth potential/scalability.

Configuration Control Board (CCB) refers to the group of technical and government representatives who recommend approval or disapproval of proposed engineering changes to a configuration change or modification. The Designated Approval Authority (DAA) provides final approval and decisions concerning risk management. (See Attachment 5)

Core hours are DARPA's standard business hours which are 7am to 7pm, Monday through Friday.

Customer Survey is the primary means for obtaining levels of customer satisfaction.

DSN is the DARPA Secret Network which consists of workstations and Windows Thin Clients with access to the SIPRNET. This network also includes standard office automation support (local printing, file services and e-mail).

DSEN (DARPA Secure Enterprise Network) will provide a highly secure, reliable, and scalable office automation based Commercial Off the Shelf (COTS) communications infrastructure capability for compartmented data communications in support of the management and administration of DARPA SAP/SAR/SCI programs based on DCID 6/3 requirements for Protection Level 3 (PL3) LAN and WAN and Protection Level 4 (PL4).

DMSS is the DARPA Management Services System, the primary unclassified data network.

DJN is the DARPA Joint World wide Intelligence Communications System (JWICS) which consists of workstations with access to DIA's JWIC's network. This network also includes standard office automation support (local printing, file services and e-mail).

E-Mail refers to a widely used Network application in which mail messages are transmitted electronically between end users over various types of networks using a variety of network

protocols. An electronic means for communication in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee.

ITIl (Information Technology Infrastructure Library) is a widely used set of best practices that provides a framework that breaks down IT functions into discrete, full-function components that spans the enterprise, called services.

LAN (Local Area Network) refers to the computer network that is confined to 3701 and 3803 N. Fairfax Drive, Arlington, VA and spans a relatively small area.

Legacy System refers to a hardware and/or software system that consists in whole (or part) of legacy applications, or uses legacy applications to achieve its transport or enabling capability.

Legacy Application refers to a software program purchased, developed or tailored specifically for use on an internal DARPA network that is owned by the Government.

MAN (Metropolitan Area Network) refers to a data network intended to serve DARPA in the Washington Metro area.

MGS (Medium Grade Service) is a managed set of Commercial Off-The-Shelf (COTS) e-mail products that utilize the DoD Medium Assurance Public Key Infrastructure (PKI). As a subset of the Defense Message System (DMS), MGS represents a set of Internet standards agreed upon by government and industry. It uses Simple Mail Transfer Protocol (SMTP) for messaging services, Lightweight Directory Access Protocol (LDAP) for directory services, Secure Multipurpose Internet Mail Extension (S/MIME) for data encryption and digital signatures, and PKI certificates, currently smart cards at DARPA, for individual identity. MGS will provide secure, interoperable messaging in an open, multi-vendor environment.

Necessary security features means those security features that are directed by DoD or Federal Government or mandated by law or regulation or as determined by DARPA. When questions of the interpretation of the requirements are necessary, DARPA shall consult with the contractor but DARPA shall be the final arbiter.

Off-site Storage refers a location of sufficient distance from DARPA to assure survival of the material in case of disaster or emergency events. The off-site location shall be approved and accredited by the Director, Security and Intelligence, DARPA.

Responsiveness refers to latency, throughput, training, interoperability, customer service, adaptability to stress, restoration time, time to increase/enhance capability, and technical refresh rate.

Seamless refers to the ability to function effectively without loss of capability.

Security Features – see Necessary Security Features

Security Requirements refers to all applicable DoD, DARPA, Director Central Intelligence Directives (DCID), National policies, and DoD requirements for collateral, sensitive compartmented information (SCI) and special access program (SAP) and as further defined by the DARPA DAA or the Director, Security and Intelligence, DARPA.

Service Delivery Point (SDP) refers to the hardware, software, and security features (e.g. smart card technology) necessary for DARPA users to perform computing functions, to access computing resources and to receive the Customer Information Technology services described in section 5.2 of this SOW. Data Seat Service Delivery Points configurations (hardware and software) are proposed by the vendor and reviewed and approved in accordance with the Configuration Control Board (CCB) defined in section 5.2 of the SOW.

Service Level Objective (SLO) is a specified level of service included in Section J as Attachment 2.

User Account refers to authorized access to the specified service exclusive of the hardware and LAN drop. User accounts shall be aggregated at the enterprise level for billing purposes.

WAN (Wide Area Network) refers to a communications network that covers a wide geographic area, such as state or country.

5.0 Statement of Work

5.1 DARPA Service Delivery Points (SDPs)

The contractor shall provide services with security features to a range of end points that include data, video conferencing center and printer seats; the DARPA classified enterprise infrastructure, and external networks for interface with commercial and other Department of Defense (DoD) communications environments. The contractor shall provide support for DARPA Service Delivery Points inside the DARPA enclave and defined locations.

A service delivery point (SDP) comprises the hardware, software, and security features (e.g. smart card technology) necessary for DARPA users to perform computing functions, to access computing resources and to receive the Customer Information Technology services described in section 5.2 of this SOW. Data Seat Service Delivery Points configurations (hardware and software) are proposed by the vendor and reviewed and approved in accordance with the Configuration Control Board (CCB) defined in section 5.2 of the SOW.

5.1.1 Data Seats

A data seat is comprised of the hardware, software, security features and services provided to DARPA users as computing resources. The data seats are defined as follows:

A. Data Seats SDPs

1. Data Seat Stand Alone - Fixed SDP capable of performing local computing functions without access to shared network resources
2. DSEN Data Seat - Fixed SDP capable of performing local and network computing functions with access to the DARPA Secure Enterprise Network (DSEN)
3. DSEN Portable Data Seat - Portable SDP which may be used to access the DSEN, or other networks. The portable data seat includes docking station or port replicator technology capable of connecting alternative input (i.e. keyboard, mouse) and output (i.e. monitor) devices
4. DJN Data Seat – Fixed SDP capable of performing local computing functions with access to DJN shared network resources
5. DJN Portable Data Seat - Portable SDP which may be used to access the DJN, or other networks. The portable data seat includes docking station or port replicator technology capable of connecting alternative input (i.e. keyboard, mouse) and output (i.e. monitor) devices
6. DSN Data Seat – Fixed SDP capable of performing local computing functions with access to DSN shared network resources
7. DSN Portable Data Seat - Portable SDP which may be used to access the DSEN, or other networks. The portable data seat includes docking station or port replicator technology capable of connecting alternative input (i.e. keyboard, mouse) and output (i.e. monitor) devices
8. DSN Terminal Data Seat – A Thin Client based SDP capable of performing local computing functions without local storage and with access to DSN shared network resources
9. Multiple Use Data Seat – A SDP which provides accounts, services and likely a removable hard drive and access to the DSEN or other networks and Customer IT Services for personnel (i.e. Department of Defense (DoD) government employees, contractors, or specified liaisons) who do not require a data seat for their exclusive use.
10. Network Services Data Seat - Provides DARPA authorized computing devices (i.e. desktops, workstations, portables, servers, including SDPs with non-standard operating systems), including necessary security features, connectivity to any servicing DARPA network and include all Customer IT services available for that network, with the exception of technology refresh. This seat does not include a Service Delivery Point.
11. Classified Networked Data Seat - Fixed SDP capable of performing local computing functions with access to other classified networks.
12. Classified Networked Portable Data Seat - Portable SDP which may be used to access other classified networks. The portable data seat includes docking station or port replicator technology capable of connecting alternative input (i.e. keyboard, mouse) and

output (i.e. monitor) devices

Each data seat must be available with upgrades through contractor-provided Catalog Services to augment basic functionality or support high-end, mission-essential, and/or technologically advanced functionality for DARPA users. User accounts for all data seats shall be provided that include access to the DARPA Secure Enterprise Network or other networks as applicable. Data seats shall be provided with the services described in sections 5.2, 5.3, and 5.4 of this statement of work. Each data seat supports DARPA mission-essential processes and shall include a technology refreshment rate as specified in Section 5.2.4.3 of this statement of work. Note that the contractor shall comply with current DoD regulations regarding the destruction of hard drives that contain sensitive and classified information.

To achieve the Information Assurance goals within DoD, a Smart Card reader may be necessary with Public Key Infrastructure (PKI) enabled applications to access DoD-compliant PKI credentials. The Contractor shall provide data seats with the capability, including all required software, of supporting and implementing DoD standards, including Smart Cards in accordance with the DoD Smart Card reader requirements in Section J as Attachment 4. The contractor may also provide DARPA users with Smart Cards in accordance with DoD specifications to be used with the Smart Card readers, the current DoD standard.

Scope: Data Seats
Reference: SLO 1, 8

5.1.2 Conference Room Seats

Conference room seats shall support audiovisual presentations that allow participants to conduct electronic meetings using dedicated audiovisual conferencing facilities. The services associated with these seats shall include but are not limited to: user training, Help Desk support and integrated configuration management.

The contractor shall provide enhanced support services for Government designated meetings for senior DARPA management, during core hours. The support for those meetings shall include contractor personnel monitoring the meeting schedule and providing set-up, testing, and support. Staff must be available for immediate assistance for the length of the meetings.

The contractor shall be responsible for the maintenance (i.e. projector light bulb replacement) and repair of all contractor-owned equipment. All lighting, seating (chairs, tables, room setup), and Telco services are not the responsibility of the contractor. Conference room seats shall be comprised of the hardware, software, security features and support services provided to DARPA users as resources. Conference room seats are defined as follows:

5.1.2.1 Classified Portable Conference Room Seat

The contractor shall make available a portable digital multimedia projector capable of performing automatic synchronization, tracking, image positioning, and video source detection for use both inside and outside the DARPA enclave. A portable conference seat shall include equipment and accessories (PC/Laptop connector cable, power cable, and carrying case).

Reference: SLO 8

5.1.2.2 Classified Basic Conference Room Seat

The contractor shall provide video presentation capability in government specified locations within the DARPA enclave. A basic conference room seat shall include equipment, infrastructure, and other services necessary to provide video presentations. The basic conference room seat includes a digital multimedia projector capable of performing automatic synchronization, image positioning, and video source detection, and network connectivity.

Reference: SLO 8, 9

5.1.2.3 Classified Advanced Conference Room Seat

The contractor shall provide audiovisual presentation capability in government specified locations within the DARPA enclave. An advanced conference room seat shall include equipment, infrastructure, and other services necessary to provide audiovisual presentations. The advanced conference room seat includes a digital multimedia projector capable of performing automatic synchronization, image positioning, and video source detection, video player/recorder capability (e.g., Video Cassette Recorder and DVD player), stereo sound systems, including dynamic speaker technology, and network connectivity.

Reference: SLO 8, 9

5.1.2.4 Classified Video Conferencing Center Seats

Video conferencing center seats shall consist of high bandwidth communications that provide point-to-point and continuous transmissions that allow participants to conduct visually interactive electronic meetings between one or more distant or local sites using dedicated video conferencing facilities which include video cameras, monitors, and audio and video communications, thus enabling participants to see and hear each other as if they were in the same room. Some of the features of this capability shall include but not be limited to: room cameras with full area coverage, large monitors, on-screen menus, dynamic speaker technology, far end camera control, video player/recorder capability, software distribution and upgrades, user training, Help Desk, integrated configuration management, integration and testing, and remote diagnostics. Section J, Attachment 8contains a description of the configuration of current

DARPA video conferencing seats. Video conferencing center seats shall be comprised of the hardware, software, security features and services provided to DARPA users as resources. Video conferencing center seats are defined as follows:

The contractor shall provide video communications at DARPA video conferencing center locations. An unclassified video conferencing center seat includes instruments, infrastructure, and other services to provide video-related connectivity within and external to DARPA. Unclassified video conferencing center seat service includes user training, Help Desk, integrated configuration management, and integration and testing. The contractor shall provide for connecting to DARPA-provided telecommunication services at each video conferencing center seat. The basic video seat price includes unlimited VTC usage between DARPA conferencing centers and other users. Basic video seat capabilities include interoperability over commercial digital services for conferencing with non-DARPA locations. The contractor shall provide operator services to include operator-assisted VTC setup and operation including off-hour support. The contractor price for unclassified video conferencing center seats shall include unlimited video conferencing sessions with other DARPA video conference centers and data seats. Calls to DARPA facilities and locations should be routed over the DARPA enterprise infrastructure. Calls to non-DARPA locations should be routed over DARPA-provided telecommunication services.

1. Video Conferencing Center Seat
2. Portable Video Conferencing Seat

Reference: SLO 8, 9

5.1.3 Reserved

5.1.3.1 Reserved

5.1.3.2 Reserved

5.1.4 Classified Printer Seats

A printer seat is a service delivery point comprised of the hardware, software, security features and services necessary for DARPA users to perform either local or network printing functions and to receive information technology services as defined in section 5.2 and Service Level Objectives. Printer seats must be compatible with all data seat service delivery points provided by the Contractor. The contractor shall electronically monitor printers to provide proactive service. All consumables associated with the proper functioning of printers other than media (paper, labels and transparencies) shall be provided by the Contractor. Printer Seat Service

Delivery Points shall be proposed by the Contractor and reviewed and approved by the Configuration Control Board (CCB) as described in section 5.2 of the Statement of Work.

The printer seats are defined as follows:

A. Personal Printer Seats
    1. Includes functionality to allow it to be available on a network and available to users.
    2. Color Printer (must have a manufacturer's rating of at least 6.5 ppm black and white, 5 ppm color, 5,000 pages per month, 600 dpi black and white, 1200 dpi color, and have a paper-tray capacity of no less than 150 sheets.)
    3. Black and White Printer (must have a manufacturer's rating of at least 15 ppm, 10,000 pages per month, 1200 dpi and a paper tray capacity of no less then 250 sheets, and duplex printing.)

B. Departmental Printer Seats
    1. Includes functionality to allow it to be available on a network and available to users.
    2. Color Printer (must have a manufacturer's rating at least 16 color ppm, 65,000 pages per month, 600 dpi, have a paper-tray capacity of no less then 700 sheets, and duplex printing.)
    3. Black and White Printer (must have a manufacturer's rating of 25 ppm, 150,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 1000 sheets, and duplex printing.)

C. Enterprise Printer Seats
    1. Includes functionality to allow it to be available on a network and available to users.
    2. Color Printer (must have a manufacturer's rating at least 16 color ppm, 65,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 700 sheets, and provide for duplex printing.)
    3. Black and White Printer (must have a manufacturer's rating of 32 ppm, 150,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 1000 sheets, and provide for duplex printing.)

Printer seats shall be provided with the services described in sections 5.2, 5.3, and 5.4 of this statement of work. Each printer seat supports DARPA mission-essential processes and shall include a technology refreshment rate as specified in this statement of work.

Reference: SLO 1, 8

5.1.5 DARPA Secure Enterprise Infrastructure

5.1.5.1 DSEN

The contractor shall provide accredited enterprise infrastructure services that are transparent to DARPA users but are essential to DARPA network functionality, security, performance, and interoperability. "Infrastructure service" refers to the various management and operational activities, hardware, software, encryption, and transmission media necessary for the delivery of services specified in sections 5.2 and 5.3 of this statement of work to internal and external DARPA users. Enterprise Infrastructure shall include integration of legacy systems, connectivity and transport services to, from, and among all DARPA Service Delivery Points (SDPs). The contractor shall migrate existing data into the DSEN based upon discussions and directions from DARPA. A description of the current DARPA Enterprise Infrastructure is included in Section J as Attachment 8. The contractor shall keep all equipment rooms, wiring closets, and other work areas in a clean and orderly state.

The DARPA Secure Enterprise is composed of 9 LAN stand alones (see Section J, Attachment 8). These existing systems and guest networks in DARPA are “stove-piped” and have no common interface or interconnection. The contractor shall facilitate the integration of these systems and incorporated into the DSEN community which includes government and contractor locations that support DARPA. The implementation may not prohibit growth or impede progress towards DARPA’s objectives.

DSEN shall provide a highly secure, reliable, and scalable office automation based Commercial Off the Shelf (COTS) communications infrastructure capability for compartmented data communications in support of the management and administration of DARPA SAP/SAR/SCI programs based on DCID 6/3 requirements for Protection Level 3 (PL3) LAN and WAN. The PL3 LAN/WAN shall not preclude future DARPA PL/4 implementations and integrated path to Protection Level 4 (PL4) capabilities. This infrastructure shall provide the interface with legacy and guest systems as required.

DSEN shall provide secure information exchange between all users on the network in accordance with the requirements of DCID 6/3. This network requires (as defined in DCID 6/3):

Confidentiality – High
Integrity – Medium
Availability - Basic

DSEN PL-3 users shall possess a Top Secret clearance, shall be DCID 6/4 and SAP eligible, and shall possess one or more SAP accesses. The desired connectivity is such that users should be able to communicate within DARPA and with other secure nodes connected to the DSEN at their common access level. Connectivity between the DSEN and non-DSEN SAP/SAR networks for data queries initiated from DSEN shall be via accredited gateways. The system shall:

a) Provide communications capabilities that support inter-site and intra-site connectivity using open systems standards,

b) Integrate legacy and new databases in a cost effective manner,

c) Integrate legacy communication systems in a cost effective manner, and

d) Provide growth flexibility to accommodate future communication requirements in a building block fashion. Future technology insertion may include advanced security features and authentication methods and technology, and voice and video telecommunications services.

The DSEN infrastructure shall utilize a cost effective topology that may be a mix of existing DOD networks, private networks, and public networks. DSEN shall provide:

a) A gateway capability for legacy mail systems (where needed with interface specifications provided),

b) Hardware/software to implement a security architecture allowing the exchange of information between LANs and WANs and provides multiple layers of defense (Defense in depth),

c) Centralized Identity Management (for example via X.500 Directory Services)

d) Centralized data repository (via database that allows metadata tagging and transfer of legacy data)

e) Media interface equipment,

f) Selected telecommunication media,

g) Gateways for network entry of Deployable nodes, and

h) A Network Operations Center (NOC) (see 5.2.4.1.1) with a Security Operations Center (SOC) (see 5.3.2.1 for more details).

i) An interface for scalable collaboration tools

Network nodes can be characterized as fixed sites. Fixed sites generally contain several Local Area Networks (LANs), each operating in dedicated/system high mode with different accesses; e.g. one LAN may be at TS/"A" and another LAN may be at TS/"A"/"B". A fixed site may be involved in one program or study and, therefore, consist of one LAN. Fixed sites are a mixture of government and contractor sites supporting a secure e-business environment.

DARPA has a legacy PL4 system. Interface with this system is to be evaluated during work accomplished in Option 1 with a full implementation during Option 2.

DSEN shall be scalable in order to allow future technology insertion and upgrades to VoIP, Video Tele-Conferencing (VTC), automated business processes (workflow), other industry collaborative databases (i.e. DOORS) and integration of guest systems like, but not limited to, JWICS, GWAN, etc. The Economic Order Quantity (price break) must be considered at the appropriate point during all the phases.

DSEN shall interface/integrate to LANs and aggregate the communication into cost effective infrastructure for the DSEN. The network shall provide the required connectivity and sufficient bandwidth to support the DSEN community. Telecommunications circuits shall be consolidated into a cost effective infrastructure with a centralized process for requests and procurements. As

new technologies (i.e. bandwidth on demand) mature, they shall be employed as appropriate to support business requirements.

DSEN shall be implemented using Commercial-Off-The-Shelf (COTS) and Government off the Shelf (GOTS) elements to the maximum extent possible. Operation and utilization of the network and its' provided services shall be as transparent to the end user as possible.

Contractor shall provide options and timelines for simultaneous or sequential implementations of the phases. The DARPA Secure Enterprise Infrastructure implementation shall take place as outlined below.

Reference: Inherent in all SLOs

5.1.5.1.1 Base Year

Deploy an accredited Top Secret/SAR/SCI PL3 LAN (called the DARPA Secure Enterprise network (DSEN)) for DARPA users and supporting contractors to enable business processes, internal to the DARPA headquarters N. Fairfax Drive, Arlington VA, 22203. The contractor shall demonstrate that the proposed PL3 solution required by this contract has been previously accredited and has wide acceptance in both the SAP and SCI communities. The scope of the deployment shall include providing a design for government approval and implementing the new infrastructure. During this deployment, the contractor shall continue to maintain the existing DSN, DJN, and other DARPA classified systems.

The contractor shall be asked to evaluate and begin to implement interfaces to the legacy PL4 network based on information provided by DARPA. The legacy network uses a Trusted label interface for bi-directional connectivity from the future PL3 system to SMTP and HTTP services over the existing Trusted enclave. Upon award of the contract an interface control document will be required to ensure label integrity between both networks. The integration between DSEN and the legacy PL4 will be funded by an EA.

5.1.5.1.2 Option Year 1

Deploy an accredited Top Secret/SAR/SCI PL3 LAN & WAN connecting existing classified seats, internal, external, fixed sites and deployable nodes with connectivity to legacy PL4 systems. The Contractor shall provide connectivity based on security and performance requirements in this SOW. The contractor shall be responsible for deployment of seats externally (fly away) to support unplanned mission needs for up to one year. During this objective, the contractor shall continue to maintain the existing classified networks. The contractor shall complete implementation of interfaces to the legacy PL4 network, details of which will be provided to all Offerors in the competitive range.

5.1.5.1.3 Option Year 2

Evaluate and develop a plan for a completely integrated infrastructure within DARPA with access to JWICS and SIPRNET, integration of applicable legacy systems (see Section J, Attachment 6) and provides at least a PL4 capability.

5.1.5.1.4 Option Year 3

The contractor shall operate and maintain DSEN, DSN, DJN, and other DARPA class systems.

5.1.5.1.5 Option Year 4

The contractor shall operate and maintain DSEN, DSN, DJN, and other DARPA class systems.

5.1.6 External Networks

The contractor shall provide external network services that are transparent to DARPA users but are essential to DARPA telecommunication functionality, security, performance, and interoperability. "Network service" refers to the various management and operational activities, hardware, software, connection service, and transmission media necessary for the delivery of telecommunications services to internal and external DARPA users as specified in sections 5.2 and 5.3, and/or ordered from section 5.4 of this statement of work. External Networks shall include connectivity and transport services to, from, and among all DARPA Service Delivery Points and other non-DARPA organizations. A description of the current DARPA External Networks is included in Section J as Attachment 8.

Reference: SLO 1, 4, 8

5.1.7 Introduction of Potential Service Delivery Points (PSDPs)

A DARPA customer can initiate the introduction of a PSDP by requesting it via the contractor-supplied catalog. If the government determines there is a requirement for the requested PSDP, the contractor shall provide all necessary documentation to the Configuration Control Board (CCB), and an Expert Assistance Task (EA) will be created for the procurement of the PSDP and interoperability and integration testing. If the PSDP is approved by the CCB, the contractor shall add it to the COTS Catalog. The government will then place a COTS catalog order on behalf of the requesting DARPA customer, and the contractor shall deliver the PSDP to the customer. If the customer cancels the order, the PSDP is not classified as a SDP (See Section 5.1), or the DP cannot be returned to the original vendor, it shall be retained as an in-stock item; its disposition shall be reflected on the Credit/Asset report, and it shall be available to the Government until fully depreciated.

The contractor shall not alter the configuration until it is determined to be in the best interests of the government, the contractor shall propose a Contract Line Item Number (CLIN) for the PSDP. If the government approves the CLIN, the contract shall be modified to include the new seat CLIN and seat order. In the event no CLIN is created for the PSDP, the contractor shall make the PSPD available for ordering from the COTS catalog.

5.1.8 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
Individual Tech Office Asset Inventory Report	Data shall include assigned office, government or contractor, onsite/offsite, name, CLIN, item description, catalog item description, cost, quantity and if applicable, bar code	Available on-line, real time, continuously commencing at the end of transition On-line, real time

5.2 Customer Information Technology (IT) Services

DARPA Customer IT Service Elements are arranged in seven Service Categories. These categories include Basic User Services, Help Desk Services, Communications Services, Systems Services, Information Assurance Services, Logistics Services, and Program Management Services. These services are necessary to provide basic functionality and shall be included in all Service Delivery Points as basic services.

Each of the seven Service Categories is described below along with their constituent Service Elements. For each, there is a brief description of the service. The description is followed by identification of the scope of the service (Scope) and a list of Service Level Objectives (SLO) contained in Section C-4 of the basic contract which are significant components the Government will use in evaluating contractor performance in delivery of these services to the DARPA customer.

5.2.1 Basic User Services

The contractor shall provide the following services to each DARPA user. The current DARPA hardware and software is defined by the Configuration Control Board (CCB) and approved by the DARPA DAA or designee for risk management and accreditation.

5.2.1.1 Standard Office Automation Software

The standard data seat integrated software suite shall include at a minimum, word processing, spreadsheet, presentation graphics, project management, database, calendaring, a collaborative work environment, forms processing, browser, and virus protection tools. For planning purposes the contractor should expect to provide equivalents to all software listed in Section J, Attachment 8. The data seat shall provide the capability to view, hear, manipulate and manage information consisting of text, graphics, images, video, and audio. This shall also include processing and rendering of the multimedia data being transferred from any source. COTS software to support advanced and/or specialized functions beyond those provided as standard office automation tools shall be available and may be purchased separately from contractor catalog services.

Scope: Basic service requirement for all Data and Video Conferencing Center seats.
Reference: SLO 8, 9

5.2.1.2 E-mail Services

The contractor shall provide services for sending, storing, processing, and receiving e-mail and multimedia e-mail attachments. The services shall be configurable to provide Medium Grade Service (MGS) capability for sending and receiving signed and encrypted e-mail and attachments, by utilizing the DoD standard, currently Public Key Infrastructure (PKI) compatible user certificates, and interoperable with MGS systems outside the DARPA domain. MGS shall be provided with e-mail packages that support cryptographic functions from a smart card or other DoD standard. Each seat should be supplied with e-mail capability and file transfer management tools. E-mail is an integral part of DARPA, and shall conform to industry standards (e.g., SMTP, native RPC, HTTP, IMAP4) for interoperability and remote access and comply with DARPA conventions for domain naming (i.e. retention of DARPA.mil domains). The contractor shall ensure that foreign nationals are clearly identifiable in electronic communications in accordance with DoD Directive 5230.20. DARPA currently imposes no quotas for users on file storage or e-mail storage.

Scope: Data and Video Conferencing Center seats.
Reference: SLO 2, 4, 8

5.2.1.3 Directory Services (DS)

The contractor shall provide and maintain global information services delivering a distributed computing environment that supports the management and utilization of file services, network resources, security services, messaging, web, e-business, white pages, and object-based services across DARPA, **as appropriate and approved by the DAA,** for the classified environment under DCID 6/3 requirements. Information services shall include storing, updating, and

publishing directory information from multiple systems (including legacy systems) and formats including office numbers, e-mail addresses, commercial, fax and telephone numbers, and contractor provided wireless phone numbers, certificates, addresses, applications, network devices, documentation and routing information, as well as other data and/or resource in support of the DARPA IT environment to multiple systems. The contractor shall ensure directory entries conform to Government standards and provide the flexibility to include users not directly supported by the contractor in Directory Services (DS). DS shall support the ability for end users to interact with the network directory services in a transparent and consistent manner.

The DS should support and facilitate the following basic functions:

1. Supported by PKI authentication services, provide the capability for users, devices, and applications to discover and utilize global information services data. Office numbers, telephone, fax numbers, and e-mail addresses shall be maintained, current and available to all DARPA personnel,

2. Support the monitoring of administration and management of network resources.

3. Support the implementation of global account management and subsequent authentication and authorization to data maintained in the global directory service.

4. Support the enablement and distribution of applications.

5. Provide a proactive environment that builds and manages relationships between objects within the global directory service.

Scope: Basic service with all data and video conferencing center seats.

Reference: SLO 1, 2, 4, 5, 8

5.2.1.4 Fax Services

The contractor work to provide the capability and features, to include security features that allow users to send outgoing faxes and receive incoming faxes via routing through email. For outgoing faxes, the contractor shall provide for automatic generation of a user-defined outgoing fax cover sheet from DARPA users from any fixed or portable seat type, and the transmission of a fax based on selection of an electronic file as an attachment to the fax cover sheet. Incoming faxes shall be routed to the DARPA user recipient via email.

Scope: Basic service with all data and video conferencing center.

Reference: SLO 1, 2, 8

5.2.1.5 External Network Access and Services

The contractor shall provide the capability and features that allow users to access in-house and external web content. The contractor shall provide communication with web host servers on DARPA secure networks and external networks as appropriate.

Scope: Basic service with all data and video conference center seats.

Reference: SLO 1, 8

5.2.1.6 Connectivity to Copy Services

The contractor shall provide connectivity to government-furnished printing and duplicating machines to enable high-speed and quantity printing services. The DARPA current standard duplicating machine is a Xerox Docutech Document Center Model 4605T.

Scope: Basic service with all video service center seats and data seats when attached to the DARPA enterprise infrastructure networks.

Reference: SLO 1, 4, 6

5.2.1.7 Reserved

5.2.1.8 Reserved

5.2.1.9 Electronic Library

The contractor shall provide Electronic Libraries on the network within the constraints of security requirements. The libraries shall have secure search and retrieval functionality. There are 15,000 existing records and approximately 4,000 additional records created each year. The libraries shall be able to attach PDF files to the records. The contractor shall facilitate the transfer information from existing media (including Bernoulli drives).

Scope: Basic service for all personnel.

Reference: System requirements for DSEN dated 25 July 2005.

5.2.1.10 Desktop Access to Government Applications

All legacy systems and applications in operation at the time of order shall continue to function as at the time of order. These systems and applications include desktop-loaded and server-hosted applications for financial and personnel functions. Contractor shall provide data seat interface and enterprise infrastructure service for legacy applications. COTS software beyond that provided by the vendor as standard office automation may be purchased separately under contractor COTS catalog. To provide solutions to fulfill emerging requirements for software re-engineering, transition of legacy applications or development of new applications, technical services may be ordered under the contractor provided Expert Assistance Catalog. Applications and functionality obtained from the contractor Expert Assistance Catalog must be integrated into and function seamlessly within the DARPA information technology environment.

Scope: Basic service with all data and video conferencing center, and seats.

Reference: SLO 1, 8, 9

5.2.1.11 Moves, Adds, Changes, and Deletes (MACDs)

When approved by DARPA, the contractor shall provide services to perform user-requested system hardware and software changes of data, video conferencing center, and/or printer seats. This applies where service within this statement of work exists.

MACDs include the following:

- De-installation, move, re-installation, or change of data or video conferencing center hardware.
- Changes in classification or protection levels of the system
- Creation, modification or deletion of a user account including email and directory services.
- A change in service delivery point type.
- A contractor periodic or unscheduled software refresh or update.
- Application of appropriate security features.

Scope: Basic Service with all data, video conference center and printer seats. For planning purposes, three user-requested MACDs per year are anticipated for each ordered data seat. User requested moves of video conferencing center seats are not anticipated but two MACDs should be anticipated.

Reference: SLO 8, 9

5.2.1.12 Software Distribution and Upgrades

The contractor shall provide the capability to distribute new and upgraded software with the method of installation and distribution resulting in transparency of functionality from the end-user perspective in accordance with best business practices and the schedule specified in the SLOs identified below. All software distribution plans and customer notifications must be approved by the Government prior to deployment. The contractor shall develop and implement a plan to update remote equipment, including equipment with personnel on travel. Software upgrades shall adhere to the Configuration and Change Management. This capability includes COTS software, GOTS software, custom applications software developed by other parties and integrated by the contractor, and deliverables ordered from contractor catalog services.

Scope: Basic service with all data, video conference center and printer data seats, enterprise infrastructure and external networks.

Reference: SLO, 8, 9

5.2.1.13 User Training

For each change in services and/or applications, the contractor shall analyze, identify, and implement the form of training most effective and efficient for DARPA users. Types of training are expected to include: desk-side, formal classroom, on-line (including Web-based FAQs for self-help on all new hardware and software deployed Agency-wide). Space for classroom-based user training shall be provided by DARPA in government or contractor-occupied facilities. Hardware, software, equipment, training materials, and supplies necessary for effective training shall be provided by the contractor. Automated user training solutions used by the contractor shall incorporate advanced distance learning solutions. User training shall be made available as a result of the following for all data, video conference center, and wireless seats including, as a minimum:

Initial Implementation

Implementation of a change in technology or user interface

Identification of user knowledge shortfall (e.g. as a result of a Help Desk call or user-invoked systems failure)

Trend Analysis performed on Help Desk tickets

Move/Add/Change

Annual security training requirement for users, to include user agreements

Trusted Download Procedures

Upon contracting officer representative (COR) request

Scope: Basic service for all data and video conference center seats.

Reference: SLO 8, 9

5.2.1.14 PKI

5.2.1.14.1 Classified PKI

The contractor shall support PKI certificates.

5.2.1.15 Reserved

5.2.1.16 Web Hosting Services

The contractor shall provide internal and external web hosting as a service for DARPA SIPRNET web site and DSEN, including storage and processing of web content. This service includes internal access, external access and classified hosting as directed by DARPA. Identification and Authentication (I&A) and Access Control to DARPA as well as to DARPA and DoD secure websites shall occur via DoD PKI compatible certificates. As part of this service, the Contractor shall provide statistics regarding web access. The service does not include authoring of web content and application development, although those services may be ordered under the contractor provided Expert Assistance Catalog.

Scope: Basic service for enterprise infrastructure.

Reference: SLO 1, 4, 6

5.2.1.17 Shared File Services

The contractor shall provide the ability for users to store and retrieve files on shared, controlled access storage media. This includes access controls, and back up and recovery. DARPA currently imposes no quotas for users on file storage or e-mail storage.

Scope: Basic service for all data seats.

Reference: SLO 1, 2, 4

5.2.1.18 Retention of DARPA Electronic Records

The contractor shall provide for retention of electronic information files as requested by the Government and consistent with applicable DoD Standard 5015.2-STD and the National Industrial Security Program Operating Manual (NISPOM).

Scope: Basic service for all data seats.

Reference: SLO 1, 2, 4

5.2.1.19 Disaster Recovery Services

The contractor shall provide a disaster recovery plan, approved offsite secure storage of data and files, and training for DARPA personnel, subject to Government approval. The contractor plan should include recommendations on the following: identified critical equipment, redundancy requirements, recovery time, failover and annual testing and review schedules. The contractor shall implement industry best practices, DCID, DoD policy and the provisions of the National Industrial Security Program Operating Manual (NISPOM). This requirement covers partial loss of service and is intended to be a part of the Agency's Continuity of Operations Plan (COOP).

Scope: Basic service for all data seats.

Reference: SLO 2, 4

5.2.1.20 Continuity of Operations Plan (COOP)

The contractor shall provide written and oral input and participate in the planning regarding the creation of a COOP.

5.2.2 Help Desk Services

The contractor shall provide an on-site Help Desk based on IT Infrastructure Library (ITIL) best practices (including Service Request, Incident and Problem Management processes) with customer-centric, courteous, responsive (most calls answered by the third ring) and knowledgeable user technical assistance for solving information technology service-related issues to the user's complete satisfaction. This process shall be implemented with full awareness of the necessity for compliance with security requirements. This includes providing an integrated service with a single point of contact for all DARPA users. ITIL best practices include, but are not limited to the following policies:

- Help Desk analysts shall retain "ownership" of each request they open until its resolution; managing hand-offs, providing follow-up, and regular customer notifications.

- Help Desk analysts shall receive on-going customer service and technical training
- User expectations shall be managed by setting and maintaining promised schedules
- Re-opened tickets shall be tracked, and trending should be performed.
- Protection of privacy information
- A Help Desk Operations Manual shall be developed and maintained covering support requirements and Standard Operating Procedures.
- A Help Desk Management System (HDMS) shall be employed. (The contractor may assume the legacy system from the incumbent or develop and implement its own at no additional cost or service impact to the Government.)
- The HDMS shall be used to develop and maintain a knowledge base of known errors and problems, including resolutions.
- The HDMS should include an audit log of all changes recorded.
- Contractor shall develop and submit to the Government for approval a HDMS user interface design and data dictionary to ensure that all desired information is captured.

The HDMS shall allow write privileges to Government specified personnel; read privileges shall be made available at the Government's discretion to personnel for validation and verification activities.

DARPA users shall have the capability to interact or communicate with the Help Desk by voice, email, fax, web and/or by personal visit to an onsite help desk located in DARPA-provided office space. Services in this contract are 24 x 7, however the predominant amount of service tickets are generated during DARPA's core hours between 7am to 7pm. Staffing requires knowledgeable analyst support to maximize first call resolution. In addition, Help Desk Services shall include junior and mid-level support for service requests that extend beyond the basic user services and problem resolution associated with Help Desk support. These service requests shall be supported and documented within the automated support request system. Examples of these types of service requests include, but are not limited to, the following:

- Virus scanning of disks
- Burning of CDs
- Data copies/moves/conversion/organization/migration
- SW/HW installation and re-configuration
- Trusted Downloads

The contractor shall identify and define the level of effort required for any service requests that necessitate engineering services that extend beyond the Helpdesk support and service request spectrum. The contractor shall provide escalation services with procedures to be reviewed and approved by DARPA and implemented by the contractor. These services shall include the timely notification of DARPA personnel by the Help Desk of planned or unplanned system maintenance or degradation of DARPA's information technology services. Because Help Desk service is mission-essential for the DARPA user community, the contractor must provide a high caliber of service and support. The provisions of FAR 52.237-3 (c) applies to the incumbent

contractor.

Scope: Basic service for all users.
Reference: SLO 8

5.2.3 Communications Services

The contractor shall provide systems services with security features in accordance with the requirements in the following subparagraphs.

5.2.3.1 Metropolitan Area Network (MAN) and Wide Area Network (WAN) Connectivity

The contractor shall provide metropolitan area network (MAN) and wide area network (WAN) connectivity between geographically separated DARPA users and devices. Such service shall provide connection to current DARPA locations identified in contractor submitted reports to meet the requirements of Section 5.2.4.5. Although Voice over IP (VoIP) is not a current offering at DARPA, contractor shall plan and make acquisitions with the knowledge that VoIP may be a requirement in the future. Additional network connection services needed in the future may be ordered from contractor provided catalog services. The provisions of FAR 52.237-3 apply to the contractor.

Scope: Basic service for Enterprise infrastructure and external networks.

Reference: SLO 1

5.2.3.2 Local Area Network (LAN) Communication Services

The contractor shall provide the capability to interconnect geographically co-located and separate DARPA Classified Local Area Networks (LANs) and attached devices. Although Voice over IP (VoIP) is not a current offering at DARPA, contractor shall plan and make acquisitions with the knowledge that VoIP may be a requirement in the future. The current LAN configuration is provided in Section J as Attachment 8.

Scope: Basic service for Enterprise infrastructure and external networks.

Reference: SLO 1

5.2.4 Systems Services

The contractor shall provide systems services with security features in accordance with the

requirements in the following subparagraphs.

5.2.4.1 Network Management System (NMS) Service

The contractor shall provide services that include fault management, configuration management/asset management, account management (for empirical user data and fiscal accountability), performance management, and security management. These services shall be provided in accordance with the Service Level Objectives in Section C-4 of the basic contract. The contractor shall make available to designated Government entities, near real time information feeds to support Government oversight, conduct security functions, maintain accessible historical data, provide summary management reports that detail the NMS functions, and allow DARPA and the contractor to forecast its future networking requirements through the use of modeling techniques. In order to meet these requirements, the contractor shall provide the following services:

5.2.4.1.1 Network Operations Center (NOC)

The contractor shall provide a Network Operations Center which shall operate 24 hours a day, seven days a week, 365 days a year. The NOC shall provide network monitor and troubleshooting, notification, router and network device management (including devices and applications through which users connect to the network remotely), and performance monitoring on DARPA networks. The NOC shall also provide performance, fault, configuration, security management, and accounting management to maintain the network and restore services in the event of an outage. The emphasis shall be security operations. The contractor shall provide and enhance GFE network management tools to monitor the health of the end-to-end network and as a basis for providing reports to the Government. NOC personnel shall follow contractor-issued, Government-approved escalation procedures for specified events and outages, which may include notifying Government personnel. The NOC shall contain an integrated Security Operations Center (SOC) (see 5.3.2.1 for details). The NOC shall be considered a part of the Mission Support functional area for the purposes of availability. The NOC shall not impede the delivery of network services in the event of a failure of the NOC. The contractor shall provide the following monthly and quarterly reports to the Government and its designees:

- Summary of network availability and problems encountered
- Detailed failure analysis and corrective actions applied for all network events that lasted 15 minutes or more, including at a minimum the following:
    - Event description, including network impact
    - Event date, time and duration
    - Services affected
    - Information on how the event was detected
    - Corrective actions
    - Root cause analysis
    - Preventative actions taken
    - Date and time Government was notified

Scope: Basic service for all Enterprise infrastructure and external networks.

Reference: SLO 1, 6, 12

5.2.4.2 Operational Support Services (OSS)

The contractor shall provide services that include, but are not limited to, data backups and recovery, data archiving, routine database audits and maintenance, log retrieval and audits, purging of records, and network address administration. The contractor shall support Government oversight, maintain accessible historical data, and provide summary management information that details the OSS functions. Network operations dashboard shall be provided to users authorized by DARPA, as designated by COR, on a real-time basis, indicating, at a minimum, the status of network assets, network performance, Internet connectivity, servers and routers. The dashboard shall be available to authorized users at any data seat connected to the DARPA network. The contractor shall develop and maintain a Backup and Recovery Plan, and submit it to the Government quarterly for review and approval. These services shall include legacy systems as requested by the Government.

Scope: Basic service for DARPA Enterprise infrastructure.

Reference:

5.2.4.3 Technology Refreshment, Insertion, Enhancement and Capacity Planning

The contractor shall provide capabilities to support the technological evolution and planning of changes to the DARPA infrastructure, specifically to estimate future requirements, capabilities, volume, usage, and application characteristics, as well as integration of emerging technology to meet the evolving requirements of DARPA. These capabilities shall be provided for all service delivery points, and include periodic analysis of enterprise infrastructure and external network capacities in consultation with DARPA regarding security requirements, along with recommendations for future engineering changes. The Technology Refreshment process shall include an analysis of customer needs and requirements, including coordination with legacy system and application owners. The contractor shall review legacy hardware on a semi-annual basis, and make recommendations on the need for replacing hardware. Customers will have the option to refuse refresh with Government concurrence. The contractor shall submit all recommendations to the Configuration Control Board (CCB) process (as defined in Section 5.2.6.1) for Government approval. The contractor shall make every effort to ensure minimal impact to the customer during refreshment, insertion and enhancement activities. For Service Delivery Points, the contractor shall minimize downtime; if the SDP is the user's primary workstation, the contractor shall offer a temporary SDP for use while the primary workstation is unavailable. Additionally, the contractor shall ensure the accuracy of data transfer and carryover: desktop icons should be restored to the same locations, printers and drivers re-installed, personal and business files transferred, and applications re-installed.

The Service Delivery Points refresh schedule is as follows:

Fixed and portable SDPs: 24 months
Conference Room Seats: 24 months
Printer Seats: 48 months

For the fixed and portable SDPs, if the Offeror proposes that any part of the fixed and portable SDP hardware and/or software be refreshed in less than or more than 24 months, that plan must be detailed in their proposal, including benefits to the Government.

External hardware peripherals and software products acquired through the COTS Catalog and compatible with the refreshed data seat shall be migrated to the refreshed Seat. If any internal components, external hardware and/or software products are determined to be incompatible or not standard (i.e. a larger hard drive) within the refreshed data seat, the Contractor shall offer the DARPA end-user alternative solutions which provide similar or better functionality through the COTS catalog and/or the Expert Assistance service.

Scope: Basic service for all service delivery points.

Reference: SLO 1, 6, 9

5.2.4.4 Reserved

5.2.5 Information Assurance Services

The contractor shall provide Information Assurance services with security features in accordance with the requirements in the following subparagraphs.

5.2.5.1 DARPA Security Operational Services

The contractor shall provide security services for protection of the Information Systems, Information System Domains (Communities of Interest), and Information Content (at rest, in use, and in-transit) in accordance with DoD and DARPA Information Assurance policies and procedures. These operational security services shall be fully integrated with DARPA authentication services to ensure confidentiality, integrity, availability, authenticity, and non-repudiation requirements as appropriate. The contractor shall implement the necessary Information Assurance (IA) mechanisms to provide these security services, and shall conduct vulnerability assessments to validate that the necessary controls are in place to satisfy the IA requirements for DARPA. As part of implementing these security services, the contractor shall be responsible for implementing Government directed IA mandates such as INFOCONs (information operations conditions) and IAVAs (information assurance vulnerability alerts).

Implementation of IA mandates shall be accomplished within Government specified timeframes. The contractor shall also be responsible for ensuring that the DARPA infrastructure meets the requirements for certification and accreditation in accordance with DoD policy and SLOs. As part of these security services, the contractor shall make available near-real time data feeds, to include access to operating systems and networks, databases, access logs, Intrusion Defense Systems, and network tools, or provide real-time data feeds where available, to support Government oversight detailing the security operational functions. Comprehensive IA/CND requirements are provided in Section 5.3 of this SOW.

Scope: Basic for all DARPA Service Delivery Points and Services.

Reference: SLO 11, 14

5.2.5.2 DARPA Security Planning Services

DARPA requires the contractor be an active and engaged partner in planning, design, architecture, engineering, and emerging security product/tools evaluation initiatives. The contractor shall provide strategic security services for DARPA to enhance the confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall support the use of mechanisms including, but not limited to, encryption, mandatory access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The contractor shall make available in accordance with the SLO, periodic information feeds, to include access to operating systems and networks, to support Government oversight, maintain accessible historical data, and provide summary management reports that detail the security planning functions. The contractor shall conduct vulnerability assessments in accordance with DARPA direction and DoD policy. On a quarterly basis, the contractor shall propose updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments, for Government review and approval. Comprehensive Security requirements are provided in Section 5.3 of this SOW.

Scope: Basic for all DARPA Service Delivery Points and Services.

Reference: SLO 11, 14

5.2.6 Logistics Services

The contractor shall provide logistics services with security features in accordance with the requirements in the following subparagraphs.

5.2.6.1 Integrated Configuration Management (CM) and Asset Management

The contractor shall develop and implement a centralized ITIL-based configuration management control process encompassing the complete inventory of hardware, software, documentation, and processes maintained in a Configuration Management Database (CMDB). The CMDB may exist as a virtual database and extend over several independent databases, but it shall contain all Configuration Items and provide the capability to map relationships of CIs to other CIs, including systems, devices, applications, groups and individuals. The Service Catalog should be a part of the CMDB, which should also house the "as built" documentation configurations of existing systems (including network diagrams), which can be used for Certification and Accreditation. The contractor shall develop and maintain a Definitive Software Library to contain authorized and deployed software configurations, a Cable Management plan to retrofit labeling and arrangement of all exposed cables in the Computer Room, wiring closets and as necessary in conference rooms, and assist the Government in implementing an enterprise-wide change management process to encompass all changes to the infrastructure.

Contractor personnel shall participate in and provide administration and technical support for a Government-controlled Configuration Control Board (CCB) that reviews all technology refreshment, technology insertion, or technology enhancement changes proposed by the contractor for each section of this statement of work on an as needed basis. The board shall examine the benefits to be achieved for DARPA in terms of effectiveness and efficiency, effect on certification and accreditation, and assess the impact of proposed technology refreshments on contract cost. DARPA designated personnel must authorize all technology refreshment changes proposed for addition to any section of the statement of working the event the proposed change departs from the current architecture and/or product suite used within DARPA. All configuration changes shall go through the change process. The contractor shall affect no changes to DARPA's architecture and/or product suite without authorization by the CCB.

The contractor shall maintain a complete and current asset inventory database of all hardware and software, and maintain a logical relationship record of the items in the asset inventory. Changes to the assets inventory shall be reflected in the configuration management system no later than 4 hours after the change. The logical relationship record shall reflect updates no more than one hour after the change. The asset inventory database shall be accessible to the Government and its designees, and shall include at a minimum the ability to query by bar code, CLIN, assignment date, user name, and directory/office assignment. The contractor shall define and implement processes to audit and control inventory, which shall allow all contractor-owned equipment, software, devices and peripherals to be monitored and tracked. Inventory acquired through the catalog must be tracked and shall remain available to the government. Audit procedures should include desk-side visits to validate user equipment; however, visits should be done with minimal impact to the customer and should not exceed one visit annually. The Government may designate personnel to accompany contractor personnel to validate desk-side audits. The Credit/Asset report must be accessible by the Government online, be maintained in near real time, and the contractor shall provide a copy to the COR monthly.

Scope: Basic service for all service delivery points and services.

Reference:

5.2.6.2 Integration and Testing

When the contractor modifies the user's existing configuration, (e. g., during initial seat fielding, applying maintenance or technology refreshment, insertion or enhancements), the contractor shall:

(a) Minimize the time involved to complete the configuration modification to achieve the updated baseline.

(b) Test prior to deployment, and coordinate system, product, and service roll outs with the government to facilitate implementation and to minimize impact to users. Coordination with the government shall include agreement on the scope of interoperability testing and assessment of impact to DARPA users. Testing must be kept within DCID 6/3 standards.

(c) Maintain interoperability among the various seat configurations. A modification to any existing baseline configuration, which was interoperable prior to the modification, shall maintain at least the same level of interoperability after the modification is fully integrated.

(d) Maintain interoperability with extranets and relevant non-DARPA provided components of the DOD Global Information Grid. Interoperability shall not be affected by any modification of the user's existing configuration.

Scope: Basic service for all service delivery points.

Reference:

5.2.6.3 Interoperability Test Plan

The contractor shall develop an interoperability test plan and procedures that shall minimize the possibility of interoperability problems during modification of user existing configurations. The contractor shall verify that interoperability is intact upon completion of the modifications, and provide for interoperability monitoring during service provisioning.

The Interoperability Test plan shall also provide for a series of mechanisms that detect unacceptable trends in performance that indicate that the software and hardware installed, component settings, and/or procedures are not in compliance, and must be corrected to support interoperability. This test plan shall address interoperability and availability as it relates to the delivery of functionality associated with service delivery points, customer IT services, IA services, items ordered from catalog services, and work performed as part of transition services.

The test plan reporting criteria shall include a threshold level agreed to by the Government and the contractor that requires immediate notification of the Government and appropriate action by

the contractor to correct. The test plan shall be proposed by the Offeror and approved by the Government for implementation in accordance with the appropriate SLOs.

References: SLO 1, 9, 10

5.2.6.4 Critical Applications and Databases

The contractor shall provide data seat interface and enterprise infrastructure service for critical legacy applications developed and/or maintained by others that are provided by the Government. The contractor shall provide desktop access, infrastructure and other services necessary to house the applications with basic service functionality on the DARPA network. The contractor shall coordinate with legacy applications owners to ensure the smooth and uninterrupted operation of legacy applications to include legacy application maintenance and deployment privileges as delineated in the SLOs. Ongoing maintenance of legacy applications and systems shall be defined for each in agreements between the Contractor and the legacy applications' and systems' owner(s). Examples of legacy applications are the DARPA financial management system, suspense tracking system, and personnel system.

Scope: Basic service for all data seats, enterprise infrastructure and external networks.

Reference: SLO 1, 3

5.2.7 Program Management Services

The contractor shall provide program management services for the entire statement of work in accordance with the requirements in the following paragraphs.

5.2.7.1 Management and Administration

The contractor shall provide effective, efficient and responsive program and project management, financial management, and contract administration services for this entire statement of work. The contractor shall provide a management team that is responsible for interfacing with the Government and other contractors' management, formulating and enforcing work and quality standards, establishing schedules, reviewing work in progress, and managing personnel. The management team shall be dedicated exclusively to this contract. The contractor shall report the status and progress of each item of work being performed as requested, but minimally, on a monthly basis and shall submit a monthly Financial Report. The contractor shall hold in-process reviews on a quarterly basis with DARPA personnel. Items for discussion include strategic planning, contractor and government performance with respect to quality, schedule, and cost, summary review of detailed Plan of Action and Milestones (POA&M) for each initiative, metrics that portray the progress of work under the contract, a summary of the quality of work performed from the points of view of DARPA customers, and recommendations

for improvement of both the contractor and government staff to achieve more effective and efficient support of the DARPA mission.

The contractor shall develop and maintain a project management methodology for planning, control, and risk management including communicating and executing individual task requirements and resolving technical, service, and management issues and risks. The methodology shall include, but not be limited to: 1) a strategic vision to include technology and service delivery; 2) advocating the service delivery concept within DARPA; 3) resolving short notice mission critical requirements or problems; 4) a clear description of contractor organization and identification of account management (who shall be responsible for DARPA accounts and their specific roles); 5) identifying, executing, and reporting key milestones and events (both one-time and recurring that may extend beyond service level metrics); 6) providing effective and responsive planning and execution of special projects, as agreed to during the term of this order; 7) a detailed description of the management approach to providing Help Desk, network, and desktop support services; 8) management approach to formulating and enforcing work and quality standards, establishing schedules, reviewing work in progress, and managing personnel; 9) management of the infrastructure; 10) approach to managing teaming relationships with any and all subcontractors; 11) approach to developing a positive, collaborative working relationship with the Government and other Government contractors; 12) management structure, organizations, and roles and responsibilities; 13) identification of security issues and risk management process, including risks identified and mitigating strategies; 14) incentives and rewards to subcontractor(s) and teaming partners for excellent performance; 15) staffing plan including skills levels, numbers of clearances; and 16) quality control process. The contractor shall also develop and maintain a Project Management Plan (PMP) that identifies the operational and organizational relationship that shall exist between contractor and DARPA personnel. The contractor shall develop, maintain and submit for Government review a Policies and Procedures (P&P) document including, but not limited to: 1) staff conduct and security requirements; 2) all aspects of job performance, e.g., Help Desk operations, network management, asset management, and change management; and 3) security procedures. The P&P should be updated and provided to the Government quarterly. Additionally, the contractor shall prepare and submit a monthly and quarterly self-assessment.

DARPA has identified key personnel, as follows: Program Manager, Deputy Program Manager, Network Operations Manager, Security Manager, VIP Help Desk Analysts, and the Customer Relationship Manager, whose duties include: acting as a liaison between the customer and contractor, meeting weekly, and as needed, with the Government Customer Representative to gather requirements and resolve issues, and communicating service levels, services, and service expectations to customers (response and resolution times, etc.)

All DARPA-related documents created by the contractor relating to processes and procedures under the contract are owned by the Government. As such, the contractor must allow and provide capabilities for authorized Government managers and staff, as well as designated contractor's access to such documents. Authorized DARPA staff and contractors shall have full and unrestricted access to such documents. Upon request by DARPA, the contractor shall deliver and convey any/all requested DARPA files/documents, etc. to the appropriate DARPA

person or organization. Likewise, the contractor must provide on-going direct systems/automated access to DARPA files and databases. Such direct systems access shall include admin or root type access for the purpose of oversight. Management consoles must be accessible for validation/monitoring purposes. Deliverables required by the contract are government property and may be redistributed within the Agency for management or verification purposes.

Scope: Entire SOW.

Reference: SLO 6

5.2.7.2 Outreach

The contractor shall perform proactive communications and outreach with DARPA users to inform them about services provided in this statement of work. The contractor shall provide current collateral such as brochures, briefings, seminars, white papers, flyers, FAQs, web content, etc. targeted to DARPA users. The contractor shall conduct information sessions in conjuncture with the Government Customer Representative and facilitate focus groups of DARPA users on a monthly basis to provide information and receive user feedback about the information technology services provided under this statement of work. The contractor shall form a supportive and close working relationship with other DARPA contractors performing work impacted by or related to this statement of work.

Scope: Basic service for all service delivery points.

Reference: SLO 6

5.2.8 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
SLO Data Report	Data showing service levels provided for period	Monthly (due 10 working days after the end of the month)

Title	Contents	Frequency
Asset and Credit Report and Asset Management Database	Data shall include description of asset, location of asset, quantity of asset, serial number/bar code, date of report, fair market value, received date, life cycle duration, purchase order cost, purchase order number, and purchase order description.	Monthly (maintained continuously in the Asset Management Database)
Configuration Management/Diagram Reports	The documentation shall provide a systems architecture view of the DARPA network in the contractor's standard format. The documentation shall include a full description of all external interface points, to include DoD compliant technologies, protocols, and peering arrangements for external connectivity. It shall include physical and logical connectivity, and how interoperability is achieved at the interfaces. The architecture shall detail DARPA network hosting of legacy systems. Data shall include graphic architecture designs and cabling diagrams, at least to the building level.	15 days after contract award, and within 5 working days of changes
Network Connectivity Plan	Data shall include network topology showing WAN/LAN connectivity. All external interface connection points (SIPRNET, JWICS, Internet, etc.) shall be clearly annotated.	15 days after contract award and within 10 working days of architecture changes

Title	Contents	Frequency
Security Architecture	Data shall include architecture diagrams that depict how information is transferred through defense in depth boundaries 1 through 4 (e.g., from WAN connections at boundary 1 to interior destinations, down to hosts on LAN at boundary 4). Diagrams should include the proposed employment of all major network components (at a minimum in-line network encryptors, firewalls, intrusion detection systems, servers, routers, switches, load-balancers, and data path) which play a significant role in network operation, management, and security. Diagrams shall also indicate location of alternate paths and backup equipment. This includes information sources, supporting paths and capacities, any unique manipulation of data in transit, points of termination and placement of all proposed security components. The diagrams shall be in contractor format. Diagrams shall address unclassified architectures, and also any unique architectural differences associated with different types of locations.	15 days after contract award, and within 10 working days of architecture changes.
COOP	The Contractor shall provide written and oral input and participate in discussions regarding the creation of a COOP.	Delivery 45 days after Government provides overall plan, annually thereafter.
Disaster Recovery Plan	The Contractor shall provide and maintain a Disaster Recovery Plan.	45 days after contract award, annually thereafter.
Information Feeds for Government Oversight	Historical data summary and management reports detailing NMS functions in contractor format.	Continuous commencing at the end of transition to full performance

Title	Contents	Frequency
Financial/Contract Funds Report	The contractor shall report the status and progress of each item of work being performed on a monthly basis in a government-approved format. The contractor shall also report on the status of the Contract funds.	Monthly
Weekly Activity Report	The contractor shall generate a status report detailing customer relations – customer outreach, training, and survey results. There report shall also provide a brief description of any system anomalies or unscheduled downtimes that occurred during the week. The contractor shall report the status and progress of each task. The contractor shall prepare and present the status and progress of individual work assignments, as well as the status of other facets of the Contract as specified by the Government.	Weekly
Program Management Plan	The Contractor shall generate and maintain a program management plan, which shall provide the means for managing and administering the services provided in this statement of work. This plan shall include standard operating procedures, processes and methods, and security features as they apply to performance of the entire statement of work. This plan shall also include the contractor's initial assessment of the requirements in section 5.3.6 of the statement of work, and address how the contractor shall ensure ongoing compliance with this requirement.	Within 5 days after contract award. To be updated within 30 days and quarterly or more often if needed thereafter.

Title	Contents	Frequency
Management Reports	The contractor shall provide management reports for all aspects of performance under the Contract. At a minimum, they shall cover the following: o Financial, including budget o Issues to be resolved o Customer services o Program-related o Work plans o Modernization recommendations, plans, and progress o Security issues, status and progress, to include status of personnel clearances and incidents involving questionable conduct o Quality control o Automated Resource Management System and in house o Inventories o Missing, lost, or stolen inventory reports o Human resources	As requested by the COR

Title	Contents	Frequency

Contract Financial Summary Report	Recap from Previous Month
	• Contract Financial Summary
	  o Estimated Contract Value
	  o Estimated Contract Award Fee
	  o Total Estimated Contract Value
	  o Expensed
	• Contract Funding
	  o ITD Funded with Award Fee
	  o ITD Expensed with Award Fee
	  o Balance
	  o Expensed
	Contract Expenditure ReCap
	• Mod Number
	• Period
	• Funding Allocation
	• Expenditure
	• Award Fee Earned
	• Balance
	Expenditure by Elements
	• CY Expenditures
	  o Period
	  o Invoice Number
	  o By CLIN
	  o Total
	COTS Catalog Activity
	• Current Period COTS
	• Adjustments
	• Current Expenditures Total
	• YTD COTS Expense
	• ITD COTS Expense
	COTS Activity by Office
	• Office
	• Current Period
	• YTD
	• Graphic to reflect
	  o Current Period by Office
	  o YTD Trends by Office
		Monthly

Title	Contents	Frequency
Interoperability Test Plan	The contractor shall develop an interoperability test plan and procedures that shall minimize the possibility of interoperability problems during modification of user existing configurations.	Within 30 days of contract award.

5.3 Information Assurance (IA) Services

The contractor shall implement the information assurance/computer network defense requirements outlined in the following paragraphs

Scope: Basic service for all service delivery points.

Reference: SLO 12

5.3.1 General DoD and DARPA IA Policies

As specified in DoDD 5200.28 (Security Requirements for Automated Information Systems (AISs), DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation Process - DITSCAP), DoD 5200.2-R (DoD Personnel Security Program), and **as specifically directed by IA policy in DARPA references and AIS Security Policy**, all automated systems and services shall meet fundamental security requirements and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive non-classified data. The provision of all IT services in this entire statement of work shall be implemented with proper products, policies, and procedures to ensure required system certification and accreditation in accordance with this policy and DCID 6/3. The contractor shall implement the day-to-day IA services and the Security & Intelligence Directorate (SID) IA shall provide oversight and enforcement management. The Contract Security Classification Specification attached to and makes part of their contract details additional security requirements that the contractor must comply with.

Scope: Basic service for all service delivery points.

Reference: SLO 12

5.3.2 Computer Network Defense (CND) Services

The contractor shall safeguard DARPA data, information resources and Information Technology (IT) assets from unauthorized disclosure or modification ensure availability and provide protection from conditions that might interfere with, or compromise their intended use. The contractor shall use a comprehensive approach to securing critical IT assets, networks, and information systems, implement robust defenses against hackers, viruses, and other online threats, and establish formal security management practices and procedures. At a minimum, the following elements are expected to be addressed in the formal practices and procedures:

- Due diligence with respect to Security Certification and Accreditation of all sensitive systems
- Use of Defense In-Depth approach and methods
- Situational awareness, situational understanding, decisive response
- Recognition of critical vulnerabilities and blocking of attempts to exploit them
- Deep integrated strategy that addresses security at all tiers: gateway, server, and client
- Device management services with advanced internal and external vulnerability scanning and threat assessment
- Comprehensive approach to vulnerability remediation employing use of automated remediation tools when/where possible
- Advanced data mining and event correlation techniques to accurately correlate, analyze, and interpret network security data in real time
- Timely notification, coordination, interface with SID IA and security
- Web access to reports for device status, change requests, and service level performance
- Assurance and control capabilities in a common operational picture among decision makers and responsible parties
- Sustained and knowledgeable and empowered workforce

Contractor security systems shall be designed to protect data as it is created, stored, modified, displayed, moved, processed, archived and disposed of. The contractor shall make available access to all contractor collected security data such as system, firewall, sensor, logs and access to the contractor security master console and/or "dashboard(s)" to Government personnel and designees in real-time or near real-time.

Due to the dynamic nature of IT-based attacks, significant advances should be expected in CND tools and practices over the life of this contract. The contractor shall be expected to continue to offer best of breed defense products and services; therefore the requirements listed below should be considered as a baseline. At a minimum, the contractor should provide the following or equivalents:

- Network boundary/perimeter protection, including firewalls, intrusion detection systems (IDSs), and virtual private networks (VPNs)
- Security monitoring and response

- Incident management, including emergency response and forensic analysis
- Vulnerability assessment and penetration testing
- Anti-virus and content filtering services
- Information security risk assessments
- Facilitate security information sharing and workflow across traditional organizational and functional lines.
- 24x7x365 security operation services
- Monitoring and analysis of the network infrastructure, and detection and appropriate rapid response to threats
- A expert level of proficiency in tools, techniques, counter-measures in network vulnerabilities
- Vulnerability testing and penetration analyses of computers and networks
- Assistance in the development and maintenance of security policies and procedures
- Assurance that policies and procedures are implemented and enforced, through both manual and automated controls
- Management status reports and escalations on all security operation requests and problems
- Participation in the remediation of audit findings as needed
- Development and implement procedures and metrics for security operations
- Implementation of automated tools for security operations as needed
- Participation in various security activities including special projects and documentation

The contractor shall support trusted upload and download, In conjunction with the Government and its designees, the contractor shall develop data contamination handling procedures and mitigation strategies while balancing COOP requirements for offsite data storage against proper protection of data. These procedures shall include reporting of sensitive or classified information loss to the Government. The principle of Least Privilege shall be enforced for accessing sensitive or classified information or IT assets (minimal permissions shall be used, and only when required.) Separation of Duties shall be enforced (role-based access scheme shall be coordinated through and enforced by DAA; currently designated through the SID IA Office). All privileged user accounts shall be established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). Privileged User accounts require the user to have final clearances. Privileged Users shall configure and operate IA and IA-enabled technology according to DoD information system IA policies and procedures, and notify the IAO of any changes that might adversely impact IA. Privileged Users shall establish and manage authorized user accounts for DoD information systems, including configuring access controls to enable access to authorized information, and removing authorizations when access is no longer needed. SSAA or AISSP documentation shall be the responsibility of the ITSP (for systems and networks under their purview).

The contractor shall establish and maintain an on-going Security Awareness and Training Program for its personnel, identifying additional security training opportunities from:

- Trend Analysis performed on Help Desk tickets
- Changes in technology or user interface resulting from tech refresh or upgrade
- Moves/Adds/Changes/Deletes
- Contracting Officer Representative (COR)
- Individual and supervisor reporting requirements relative to security.

5.3.2.1 Security Operations Center

The contractor shall establish a Security Operation Center (SOC). Integration of the SOC with the NOC is desired. (i.e., independent NOC and SOC meet minimum requirements but integrated NSOC is preferred).

Functions required of the SOC include, at a minimum:

Firewall Management and Perimeter Protection

- Ongoing reassessment of firewall configuration and infrastructure to ensure compliance with existing inbound and outbound policies and requirements
- Assistance in implementing firewall policies
- Analyzing and reporting of firewall log results (use, attack attempts blocked, summaries, etc.
- Adding, modifying and retiring routine or emergency firewall rules
- Testing and validation of rule set changes
- Ensuring rules are applied to correct interfaces on the firewall
- Rule maintenance schedules
- Events of conditions requiring updates
- SLAs for rule changes?
- Repairs and Maintenance
- Online log and statistical reports (near real time)
- Firewall Management Reports:
  - Current status of the rules and configurations
  - Rule set maintenance and other scheduled outages
  - Results of periodic testing of the rules and alert mechanisms
  - Unscheduled Operational Outages
  - Log Trending and analysis (anomaly detection and threshold analysis)

Intrusion Detection and Prevention

- Initial assessment of the architectural infrastructure
- Ongoing assessment of the IDS infrastructure
- Timely patching and security updates to all operating systems and subsystems
- Sensor monitoring, and analysis
- Configuration, review and maintenance of IDS profiles

- On-site repairs
- Preventive maintenance including signature/profile updates, network diagnostics, equipment service, software and configuration updates, and data archival (backups, off-site storage).
- Incident Response and forensics
- Managed firewall services
- Incident Correlation
- SLAs for time to respond/time to repair
- Provide status of ongoing investigations
- Provide computer forensic support to investigations in the form of evidence seizure, computer forensic analysis and data recovery
- Intrusion Response Services to include:
    - Analysis
    - Internal and external communication with affected parties
    - Collecting and protecting information including evidence
    - Containing the intrusion to limit the damage caused
    - Eliminating all means of intruder access
    - Returning systems to normal operation
    - Conducting an intrusion post mortem meeting to discuss lessons learned
    - Implementing identified improvements to remove vulnerabilities

Miscellaneous SOC Functions

- Maintain/Operate WebSense or equivalent software
- Website access monitoring with Bluecoat or equivalent--currently tied to WebSense capability
- Spyware filtering
- Antivirus deployment and updates
- Operation/Maintenance of VPN servers
- Boundary routers (particularly those with Access Control Lists, which back up the firewall.)
- Establishment of safeguards and controls which prevent unpatched or out-of-date systems from attaching to DARPA networks or devices that might be on the system, at the VPN, or on the Active Directory servers points of entry.
- Deployment, maintenance and operation of personal firewalls that shall be deployed on the end systems, but must have rules coordinated with the enterprise firewall.
- Internal intrusion detection that must have elements deployed on workstations and servers, and the internal network in order to be effective.
- Implementation, maintenance and operation of authentication systems including interfaces or use or CAC card, SecurID, and passwords that ties into firewalls, servers, etc.
- Deployment, maintenance and operation of wireless detection systems or software controls.

- Reporting:
  - IDS-detected attacks
  - Security Incident Reports
  - Network Trend analysis
  - Incident Report and Notification
  - Current status of the signature/profile configurations
  - Signature/profile maintenance and other scheduled outages
  - Results of periodic testing of signatures, profiles, and alert mechanisms
  - Unscheduled operational outages
  - Log Trending and analysis (anomaly detection and traffic analysis)

5.3.2.2 Data Ownership, Access Rights, and Delivery

All DARPA information resources and contractor generated data such as system log data, documentation, program code, automated scripts and ancillary information under the contract is owned by the Government. As such, the contractor must allow and provide capabilities for authorized Government managers and staff, as well as designated contractors' access to such data. Authorized DARPA staff and contractors shall have full and unrestricted access to such data. Upon request by DARPA, the contractor shall, without delay, deliver and convey any/all requested DARPA files/documents, etc. to the appropriate DARPA person or organization. Likewise, the contractor must provide on-going direct systems/automated access to DARPA security files and databases. Such direct systems access shall include admin or root type access for the purpose of oversight. Management consoles must be accessible for validation/monitoring purposes. Deliverables required by the contract are government property and may be redistributed within the Agency for management or verification purposes.

5.3.3 Multi-Level Security (MLS)

Any implementation within DARPA of a MLS device such as a High Assurance Guard or MLS Web Server shall be in accordance with the guidelines established by the Defense Information Switch Network (DISN) Security Accreditation Working Group (DSAWG) and the Secret and Below Interoperability (SABI) effort and DCID 6/3 requirements. Accordingly, in cases where the DARPA infrastructure is required to interface with other sensitive networks, such as SIPRNET, integration with an appropriate cryptographic device is required. Cryptographic devices shall be provided by the government.

5.3.4 Reserved

5.3.5 Critical Government Roles with respect to IA

Although DARPA expects the contractor to pursue an aggressive strategy for design, deployment, and operation of the DARPA infrastructure, authorized DARPA personnel

(Government and contractor) must perform a number of critical security roles. These roles fall into two categories: ensuring that the security of the DARPA infrastructure satisfies DARPA, DoD, and Federal requirements and exercising essential command authority over any DARPA defensive Information Warfare (IW) activities.

The Government will furnish cryptographic equipment and keying material. The contractor shall be responsible for loading the keying material into the cryptographic equipment used to protect information using the Electronic Key Management System (EKMS) as appropriate. The contractor shall be accountable for all cryptographic material in accordance with the National Industrial Security Program Operating Manual (NISPOM). The contractor may be responsible for all shipping and handling of GFE DARPA cryptographic material to and from a DoD Crypto Repair Facility (CRF) for required depot repairs.

In concert with the requirements for Certification and Accreditation (C&A) of all DoD computer networks (classified), the DAA and his designated authorized DARPA representative shall be the approving authority for the following components of the DARPA infrastructure:

a. Security architecture
b. Configuration Management Plan
c. SSAA
d. Security Requirements Traceability Matrix (SRTM)
e. Certification Test Plan
f. Risk Management Matrix
g. Penetration Testing
h. Security critical product selections
i. Network connectivity plan
j. Security procedures
k. Other security critical factors as required

In the above role, DARPA personnel will seek to use the most expeditious procedures without compromising the integrity of the security evaluation process. Also, with respect to item (h) above, the DARPA infrastructure shall comply with the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 for the implementation of COTS and GOTS IA and IA-enabled IT products.

DARPA will use security assessment teams to conduct authorized simulated attacks against operational DARPA networks to ensure the DARPA infrastructure satisfies the security related SLOs and that DARPA, DoD, and national security requirements are met. As part of this approach, Red Teams will also conduct design, product, and configuration reviews. Red Teams will focus on identifying vulnerabilities and risk associated with operation of the DARPA infrastructure. DARPA will ensure that DARPA, DoD, and national policies and procedures are followed in conducting Red Team operations. While DARPA intends to use contractor support personnel to supplement government personnel in conducting security assessment operations, leadership of these teams shall be government based.

With respect to CND, responses to network threats and attacks constitute Information Warfare (IW) defense command decisions that as a minimum shall be authorized by designated DARPA personnel. Along this line, the DARPA command structure shall retain directive authority over all DARPA infrastructure threat responses. These DARPA personnel shall also be the conduits for authorized responses to directives received from JTF-GNO or Joint Service regional CINCs, for coordinated Joint Service response to threats. In particular, as the INFOCON level is raised, DARPA personnel shall retain command decision authority. During these periods, SLO compliance may be relaxed at the discretion of the Government.

DARPA shall be the approving authority for the security architecture since government personnel will be responsible for security critical roles and shall have to use the infrastructure for critical operations. The security architecture is the primary mechanism that underlies the criticality of the DARPA infrastructure. The overall performance of the network shall still be the responsibility of the contractor given this constraint.

Government personnel will retain essential command authority and approval authority of security changes. With the constraints outlined above, the contractor is still responsible for the overall performance of the DARPA infrastructure in accordance with the SLOs.

5.3.6 Classified Information Support

In accordance with the National Industrial Security Program Operating Manual, DoD 5220.M, the contractor must possess a Top Secret Facility Security Clearance to perform the tasks or services required on this contract. Security requirements relating to the handling and safeguarding of classified information are identified in the DD Form 254 provided as part of the contract. Contractor personnel, whose duties require access to systems processing classified information, must possess a security clearance at least equal to the highest degree of classification involved and have a validated need-to-know prior to beginning work on the classified system. All personnel who work onsite at DARPA must have a final DoD Secret clearance.

5.3.7 Sensitive Information Support (Non-Classified)

Under current Federal guidelines, all officially held information is considered sensitive to some degree and must be protected by the contractor as specified in applicable IT Security Plans. Types of sensitive information that will be found on DARPA systems include, but are not limited to: Privacy Act information, information that is proprietary to companies or contractors other than the subject contractor, information protected by International Traffic in Arms Regulation (ITAR), technology restricted from foreign dissemination, DARPA administrative communications, including those of senior Government officials, procurement and budget data, information related to Equal Employment Opportunity (EEO), labor relations, legal actions, disciplinary actions, complaints, IT security pending cases, civil and criminal investigations, and

information not releasable under the Freedom of Information Act (FOIA) (e.g. payroll, personnel, and medical data).

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments shall be forwarded to DARPA-designated personnel for a determination of personnel suitability and requirements for individuals assigned to these positions. Periodic re-evaluations of positions and suitability requirements shall be necessary during the life of the contract as positions and assignments change.

Performance under this contract will involve access to and/or generation of sensitive information or systems. The contractor shall perform an assessment to determine position sensitivity and management controls to prevent the individuals in these positions from bypassing controls and processes such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges. Ongoing reevaluations of the position and suitability requirements will be necessary during the life of the contract as positions and assignments change. Due to the sensitivity of the information, contractor personnel who exhibit characteristics of mental impairment or characteristics that indicate a lack of integrity, conduct, or attitude that brings into question their trustworthiness, shall be immediately reported to the Director Security & Intelligence Directorate, DARPA.

The contractor shall conduct risk assessments, document the results, and develop and maintain internal security plans on-line and in accordance with applicable DoD guidelines and the NISPOM. These plans shall describe how the contractor shall ensure the integrity, availability, and confidentiality of the information that it is operationally responsible to protect within the vendor's facilities and at government facilities. For example, the contractor shall ensure that foreign nationals within their corporate staff shall not have access to DARPA systems or networks or DARPA data. Release determination is solely the responsibility of the Government. The contractors risk assessments and IT Security Plans shall be updated at least every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. If new or unanticipated threats or hazards are discovered by the contractor or government, or if existing safeguards have ceased to function effectively, the contractor shall immediately notify the Government in near real time, update the risk assessments and IT Security Plans (within 30 working days) and shall make risk reduction recommendations to the DARPA system owner and the DARPA information owners (within 5 working days).

5.3.8 Privacy and Security Safeguards

The contractor shall not publish or disclose in any manner, without written consent of the Government, the details of any security safeguards designed, developed, or implemented by the

contractor under this contract. This restriction is applicable to the contractor's off-site corporate offices.

The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user, such as being reassigned, removed for repair, replaced, or upgraded, is cleared of all DARPA data and sensitive application software by a technique approved by the Government, currently overwriting at least three times. For IT resources leaving DARPA use, applications acquired via a "site-license" or "server license" shall be removed. Damaged IT storage media shall be degaussed or destroyed in accordance with the appropriate DoD or DARPA security requirements.

DARPA will carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of Government data. The contractor shall afford DARPA access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, system databases, and personnel to facilitate the audits and inspections. DARPA will conduct an audit on a periodic event-driven basis of the contractor's security management processes and procedures.

5.3.9 Certification and Accreditation (C&A)

DARPA will provide the contractor with the most current information regarding the C&A status of the existing DARPA networks that comprise the "as is" configuration of the DARPA infrastructure. The contractor shall be responsible for developing a transition plan to support the migration from the "as is" DARPA infrastructure at contract award to the contractor implemented DARPA infrastructure. The contractor shall be responsible for delivering a system that can be certified and accredited in accordance with DCID 6/3 Security Requirements. With this support, the contractor shall create a Security CONOPS, System Security Plans (AISSP's or SSAA's, as appropriate), Risk Management Matrix, Security Requirements Traceability Matrix, Certification Test Plan, Penetration Testing and support DARPA in the following phases of C&A as defined in the DITSCAP: Definition, Verification, Validation, and Post-Accreditation. During Certification Testing, all findings shall be addressed in categories and shall be resolved as directed by the DAA. Similarly, the contractor shall be responsible for supporting the Government in satisfying the DIA, NRO, DISA and NSA guidelines and requirements for connection to the SIPRNET, NIPRNET, INTERNET, JWICS and GWAN. This shall include providing a security concept of operations document, sufficient architecture documentation (including topology), a system security authorization agreement (SSAA), risk assessments, risk mitigation plans, and other supporting documents required to support accreditation. The contractor shall support DARPA in the role as certification agent.

5.3.10 DARPA Enclaves

A Community of Interest (COI) is a logical grouping of users who have a requirement to access information that should not be made available to the general DARPA user population. This

requirement can be based on specific security requirements, geographical location, unique functional requirements, or unique command relationships. To meet this requirement, a logical perimeter is established around the COI, using Defense in Depth IA mechanisms. Some examples of COIs are personnel systems (for handling Privacy Act Data), and geographically dispersed personnel handling sensitive information... COIs will be established under the authority of the DARPA Director of Management Operations (OMO) in coordination with the DAA.

The contractor shall dynamically establish, maintain, and disestablish multiple communities whose membership is dependent upon the presentation of community (enclave) credentials (PKI/keys/smart cards), as required by and in coordination with DARPA. All of the communities above the non-classified level require Type 1 cryptographic separation. However, the DAA may authorize the use of PKI and VPN technology for COI implementation within classified enclaves. Communities within non-classified enclaves require the use of PKI and VPN technology for cryptographic separation. Connection between communities requires a Government approved gateway or guard appliance and approval of the DARPA DAA.

5.3.11 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
Incident Report	Data shall include any configuration changes, computer incidents, network incidents, INFOCON status, and intrusion detection reaction alert status.	Within 24 hours of incident

Title	Contents	Frequency
C&A Documentation	Data shall include the following: o CONOPS (Concept of Operations) o System Security Authorization Agreement (SSAA) or Automated Information System Security Plan (AISSP) o Risk Assessments o Risk Management Matrix o Risk Mitigation Plans o Security Requirements Traceability Matrix (SRTM) o Certification Test Plan o Vulnerability Assessments o Penetration Testing Results	SSAA: Initial draft 30 days after contract award, second delivery 90 days after contract award, third delivery 180 days after contract award, and within 5 days of any significant architecture revisions. All other requirements due annually, at a minimum. Work closely with DAA and designated representative(s) or ISSO/ISSM.
Security Status Report	Real time or near real time data feed supporting government oversight of security functions.	Continuous commencing at the end of transition to full performance
Accreditation Letter	Proposed PL-3 solution	Delivery with initial contract award.
Security Management Practices & Procedures	Data shall include security procedures describing how IA mechanisms shall be operated to provide the security services specified in the statement of work.	Delivery with initial contract award, updates with changes

5.4 Catalog Services

Catalog services shall be provided by the contractor to provide DARPA with the flexibility to order services necessary to meet mission-essential requirements not otherwise provided as service delivery points, customer IT service, or IA service. The contractor shall provide the catalog services in accordance with the requirements in the following subparagraphs:

5.4.1 COTS Catalog

COTS Catalog services provide COTS software or hardware associated with the Service Delivery Points (SDPs), or the piloting of new SDPs that may be added to support requirements beyond the basic services. (Pilot SDPs shall be understood to be SDPs obtained for testing, by the Government, the Contractor, or a Government-designated third party.) The Contractor shall

provide a catalog of hardware, software and other COTS items to meet DARPA's need for specialized or advanced functionality to be ordered and funded as needed. Items listed in the catalog shall be pre-integrated and available for immediate access when ordered to augment services, or available for pilot purposes when ordered in conjunction with Expert Assistance tasks. All items in the catalog shall be integrated and interoperate with all services upon deployment. All items, except those that may function as SDPs, shall include the provision of all service identified in this SOW (i.e. installation, initial training, Help Desk, etc.) SDPs may obtain Customer IT services either through transitioning into Data Seats, or by ordering services via the Network Services Seat. Addition and removal of items from the catalog as well as changes in cost shall be upon the approval of the contracting officer representative. Items to be included in this catalog shall include but not be limited to the current non-standard but supported items listed in section J, Attachment 8. These items shall be available for ordering through a contractor-provided, government-approved, web-enabled catalog with multiple approval levels including partial order approval. The catalog shall publish alerts, via email, to all appropriate parties as order status changes. The catalog shall have the capability of generating live reports, including financial reports by time, status and office, and have the capability to capture funding levels by Technical Office.

In the event of a COTS catalog order cancellation, the Contractor shall, in conjunction with the Government, determine if the item(s) should be returned to the original vendor or retained as an in-stock item. If the item is returned the Contractor and the Government will determine an equitable adjustment to be reflected on the Contractor's invoice. If the item is retained, its disposition shall be reflected on the Credit/Asset report, and it shall be available to the Government until it is fully depreciated.

Reference: SLO 9

5.4.2 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
Order Status Report	Data shall include ordering office, order number, order date, order status, back order date, ordered amount due, date order created, order created by I.D., date order last modified, number of ordered products, ordered product, product number, quantity, order product status and unfilled orders status, quantity shipped, date shipped, quantity installed, and order price.	Monthly (maintained continuously)

Title	Contents	Frequency
Catalog Expenditure Report	Report shall allow for the following user enterable variables: Office, Fiscal Year, Expenditure Status (Committed, Pending Approval, Open). Data shall include ordering office, Fiscal Year, current funding level, order date, order number, order created by ID, order item, order status, cost, total by expenditure status, funds remaining. User shall be able to access any individual order via link directly from the report.	Available on-line, real time, continuously commencing at the end of transition On-line, real time
Pending Order Approval Report	Data shall include order number, order created by ID, order office, order submitted date, order status, order Fiscal Year. User shall be able to access any individual order via link directly from the report.	Available on-line, real time, continuously commencing at the end of transition On-line, real time
Pending Catalog Item Entry Approval Report	Data shall include item Id, Item Name, cost, associated order number. User shall be able to access any individual order via link directly from the report.	Available on-line, real time, continuously commencing at the end of transition On-line, real time

5.5 Expert Assistance (EA) Services

Expert Assistance services shall be provided by the contractor to provide DARPA with the flexibility to order services necessary to meet mission-essential requirements not otherwise provided as service delivery points, customer IT service, or IA/CND service. The contractor shall provide the Expert Assistance services in accordance with the requirements in the following subparagraphs:

5.5.1 EA Services

These capabilities provide services to support information technology-related requirements that may be needed to augment basic services or may be required beyond the basic services. The services shall be requested through a Government managed process. The Contractor shall

provide labor categories with pre-negotiated hourly rates for DARPA to obtain information technology services on an as-needed basis to accommodate emerging requirements. Deliverables provided under this item shall be transition-able to the basic services (i.e. installation, initial training, Help Desk, etc.) provided by this SOW if specified by DARPA. The addition and removal of labor categories shall be upon the approval of the Contracting Officer. The Contractor shall meet with the Government weekly to review the EA Project Status Report and discuss the progress of each EA task.

The contractor shall have the capability of applications development which the Government may order through EA tasks. The contractor should expect support requests, at a minimum, for Microsoft SharePoint, Computer Associates ClearPath and graphic design. Application developers should have the ability to work effectively and collaboratively with Government personnel and other Government contractors. Additionally, developers shall follow documented project management schedules, and adhere to a Quality Management process which includes peer review. All applications must be developed, documented and follow the Applications Lifecycle Development process and procedures for requirements gathering, planning, development, and implementation.

Reference: SLO 9

5.5.2 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
Weekly Expert Assistance Status Report	The contractor shall generate a weekly status report detailing new expert assistance (EA) requests and the status of current EAs, including New Technology Refreshments, Pending EA Requests, Project Delivery Dates, Projected Completion Dates, Cost Impacts, Terminated Requests, Project Change Requests, etc. In the Weekly EA Status Report the contractor shall provide a brief description of the EA request, the date the request was made, the name of the requestor and other pertinent identifiers or the EA request. (Note: The government will provide the unique project code/number for all requests deemed an EA.)	Weekly.
Initial Contract Transition Plan	The contractor shall generate and maintain an initial contract transition plan, which shall provide the means for managing and administering the orderly transition of services from the incumbent contractor to include processes and procedures.	Within 5 days after contract award.

5.6 Governance

The IT Configuration Control Governance Structure is included in Section J as Attachment 7.

5.6.1 Data Reporting

The Contractor shall electronically post the following information for on-line and/or secure Internet access by designated DARPA personnel. Reports shall be in Government-approved format. The Contractor shall post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Title	Contents	Frequency
Fielding and Implementation Plan	The contractor shall generate an implementation plan, which shall provide the means for coordinating system, product, and service rollouts and tests with the Government. This plan shall reflect the actions identified in the Risk Assessment, C&A, and Security CONOPS (including Disaster Recovery Plan) (as shown above), and Interoperability Test Plan.	30 days after contract award.
Contractor Configuration Management (CM) Plan	Data shall include organizational structure, roles, responsibilities, policies, and methods employed for configuration management.	
Configuration Change Request	Report should include, at a minimum: • Type of Request • Priority Level • Name/Organization of Requestor • Explanation of Change • Justification of Change • Impact of Change • Schedule	As needed.
Accreditation Support Documentation	The contractor shall create a Security CONOPS, System Security Plans (AISSP's or SSAA's, as appropriate), Risk Management Matrix, Security Requirements Traceability Matrix, Certification Test Plan, Penetration Testing	As needed.
Configuration Control Board Working Group (CCBWG) Technical Review and Interoperability Test Plan	Report should include, at a minimum: • Background • Executive Summary of Testing Done • Test Plan and Results Matrix • Test Summary	As needed.

5.7 Transition Services

The contractor shall provide transition services necessary to migrate current "as is" IT services to future "to be" IT services in accordance with the requirements in the following subparagraphs.

Reference: SLO to be provided as part of Offeror's proposal

5.7.1 Initial Contract Transition

The Contractor shall transition assets, services and support including all hardware, software, data, documentation and/or related material based on Fair Market Value, as determined by a Contractor-provided, Government-approved schedule, in such a way as to facilitate a smooth, professional, business-like transition to full support by the Contractor in accordance with the provisions of FAR 52.237-3, and in accordance with the transition approach incorporated by reference herein: (see Offeror's proposal transition plan). In order to provide continuity of DARPA information technology services, the Contractor shall assume full responsibility for all of the requirements in the statement of work at the beginning of the Basic period of performance, currently anticipated as (see date of full contract responsibility in Offeror's proposal). Contractor shall submit a Transition Plan as part of the proposal package. The transition plan shall detail the following:

- An approach that clearly demonstrates the ability to assume, or transfer, full contractual responsibility, to include processes and procedures, configuration management, and transfer of assets, without degradation of performance during and upon completion of the transition period.
- The hiring/availability of properly cleared (must be DCID 6/4 eligible) and qualified key personnel, scheduling of transition activities and plans for the assumption, or transference, of responsibility for information system services support functions which demonstrates the Offeror's ability to conduct the transition with minimal performance deterioration.
- The hiring/availability of a staff consisting minimally of 50 trained and properly cleared (must be DCID 6/4 eligible) individuals.

The transition plan shall identify the staff for the phase in considering the familiarization with the DARPA's objectives and scope of IT supports service requirements. If the transition plan assumes a dependency upon the incumbent contractor, please identify the depth and extent of the corporation assumed. The transition period shall last no longer than 90 days. During the period of (see Phase-in begin date in Offeror's proposal) to (see Phase-in end date in Offeror's proposal) the Contractor shall accomplish transition and training of Contractor personnel as required for the assumption of full contract responsibility. To ensure continuity of DARPA information technology service operations during transition and to assist the Offeror in achieving successful transition, DARPA will make the incumbent contractor available for a period of time not to exceed (see number of days in Offeror's proposal). To assist in transitioning explicit and tacit knowledge, methods, processes and procedures from the incumbent contractor to the successful Offeror, the provisions of FAR 52.237-3(c) apply to the incumbent contractor.

Reference: SLO x (provided as part of Offeror's proposal and as approved by DARPA)

5.7.2 End of Contract Transition

In the event this contract is terminated, expires or is superseded, the contractor shall be required to permit the government or its designee to purchase at its discretion any or all hardware, software, documentation and/or related material based on Fair Market Value, as determined by a Contractor-provided, Government-approved schedule, in such a way as to facilitate a smooth, professional, business-like transition to full support by a new contractor in accordance with the provisions of FAR 52.237-3. The contractor shall perform all activities in the subparagraphs to follow, including transition planning and reporting, and at the discretion of the government, shall be required to continue to provide services during the transition period of the follow contractor.

5.7.2.1 Material and Services

The contractor shall permit the government or its designee to purchase at its discretion any or all hardware, software, documentation and/or related material based on the current book value, according to the contractor's depreciation schedule, for any or all of the material in the possession of the government in the event this contract is terminated for any reason. Likewise the contractor shall permit the government or its designee to assume any leases at it's discretion for any equipment, software, training, materials, supplies, services or communications capabilities provided under this contract in the event this contract is terminated for any reason.

5.7.2.2 Data and Files

The contractor shall relinquish all files and documentation related to this contract, regardless of the media it is stored on (including paper, tape, diskette, CD, etc.), to the government or its designee and facilitate the migration of data

5.7.2.3 Explicit and Tacit Knowledge

The contractor shall transition all explicit and tacit knowledge related to this contract to the government or its designee. Specifically, all documentation related to this contract, including processes, plans, procedures and methods, etc., regardless of the source or technique used to acquire this knowledge, is the property of the government or its designee. Additionally, all documentation must be maintained on-line.
Reference: SLO X (to be provided as part of Offeror's proposal)

5.7.2.4 Destruction of Classified Equipment

The contractor shall destroy all equipment associated with this SOW as classified.

Reference: DoD 5220.22-M, Chap5, Sec 7.